Information Systems Audit UPDATE

Arkansas Administrative Statewide Information System General Controls

ARKANSAS
DIVISION OF
LEGISLATIVE
AUDIT

JULY 8, 2005

Legislative Joint
Auditing Committee
172 State Capitol
Little Rock, AR 72201

Phone: 501-683-8600
Fax: 501-683-8605

www.legaudit.state.ar.us

Audit No. IS0000304

This information systems audit update is being issued to update the Legislative Joint Auditing Committee (LJAC) on the status of the recommendations included in our information systems audit, *Arkansas Administrative Statewide Information Systems (AASIS) General Control*s, dated April 12, 2002.

OBJECTIVES

Our objectives in conducting the original audit were to test system control parameters as well as policies and procedures to obtain reasonable assurance that sufficient controls exist in AASIS to:

- Protect the application, database and web servers from unauthorized access;
- Provide for the continuation of computer processing capabilities in the event of an disaster;
- Ensure proper management of the computer hardware;
- Ensure that only approved and tested system control parameters are updated to the production system; and
- Adequately test and approve programs before being placed in the production system.

SCOPE AND METHODOLOGY

Our audit was conducted for the time period June 1, 2004 through March 24, 2005. We interviewed appropriate personnel from the Department of Information Systems (DIS) and the Department of Finance and Administration (DFA) as well as performed tests of controls implemented as a direct result of our original audit.

BACKGROUND

AASIS, the statewide accounting system purchased from SAP Public Sector and Education, Inc., went on-line July 1, 2001. DFA utilizes an integrated team of approximately seventy-five (75) functional and technical personnel for the management and operation of the AASIS Support Center (ASC). Currently, the ASC Director is an employee of DIS but reports directly to the Director of DFA under an exclusive contract between the two agencies. The SAP application is primarily supported by personnel with functional and configuration expertise in the business processes. These duties are performed primarily by DFA personnel.

DFA utilizes DIS to provide the technical activities including program customization, database administration, and SAP R/3 BASIS administration. DIS also hosts and supports the hardware, software, change control, operating systems, system security, connectivity, and disaster recovery contingency planning for the SAP R/3 system on behalf of DFA.

UPDATE ON ORIGINAL RECOMMENDATIONS

Our initial audit contained twelve (12) recommendations. Based upon the follow-up evidence gathered, it appears DIS and DFA have, in most cases, adequately addressed the findings from the 2002 audit. Our original recommendations as well as current updates are contained below.

1. Contingency Plan

RECOMMENDATION: A Contingency Plan includes procedures for providing hardware, software, supplies, and personnel to operate the backup computer facilities or restore the primary computer facilities in the case of a major interruption or disaster. DIS' Contingency Plan contains emergency call lists, organization charts, and procedures but does not address recovery of computer processing or backup computer facilities. This situation could cause the state to be without AASIS computer processing for an extended period of time in the event of a disaster or major interruption. We recommend the inclusion of computer processing recovery procedures in the Contingency Plan, that arrangements be made for backup computer facilities and that the Plan be tested periodically. We further recommend that DIS management make arrangements for backup computer facilities.

UPDATE: *DIS has developed a Data Center Recovery Manual that is updated weekly, and addresses computer processing recovery in the event of an outage. These procedures are tested regularly during the course of operations. Both full and partial restores have been successfully undertaken. DIS entered into a contract effective May 7, 2003 with Fidelity (via Sungard Recovery Services) for disaster recovery services including backup hardware, facilities, and technical support. The contract provides hot- and cold-site facilities, mobile recovery system, mobile and cold-site computer space, office space, and workgroup space. The contract also provides for fully technically supported annual testing periods. The monthly participation fee is $101,781. Additional costs in the event of a disaster include:*

- *$27,500 for a non-refundable declaration fee (charged if Sungard is notified of a disaster situation); and*
- *$21,750 for daily usage fees (includes daily use of hot-site, mobile recovery system and workgroup space for up to six weeks).*

In March of 2005, DIS successfully restored AASIS during the hot-site testing at the Sungard facility in Philadelphia, Pennsylvania . Individuals at the hot-site and in Arkansas performed limited transaction testing on the restored system.

For future disaster recovery tests we recommend:

- *More extensive tests of key transactions and business processes;*

- *Testing of the printing functionality;*
- *A roll forward of AASIS backups be performed to provide increased assurance that the most current data and configuration can be successfully restored; and*
- *Network restoration testing of core network devices to connect users in Arkansas to the recovery center in Philadelphia.*

Management Response: *DIS concurs with the above recommendation. Each Disaster Recovery test has been more successful. The Disaster Recovery contract provides for a limited number of hours at the Sungard facility for each test. Testing time at the Sungard Facility has been a limiting factor. DIS will ensure that the next scheduled tests addresses each of the items listed and documents the results of the tests. The next Disaster Recovery test is scheduled for September 13th, 2005 in Carlstadt NJ.*

2. Backup Tapes

RECOMMENDATION: Backup tapes of the AASIS system and data files are not rotated to an off-site storage location. This situation could cause financial data and AASIS system configuration to be irretrievably lost in the event of a disaster. Sound database management dictates that backups of critical system and data files should be stored at a remote site.

We recommend that the backup copies be periodically rotated to off-site storage.

UPDATE: *Total system backups (including master and transaction data files, operating system and production programs) are performed daily and rotated to off-site storage.*

3. Firewall

RECOMMENDATION: A firewall is a system of hardware and software components that restrict access between a network and the internet or between other networks. A firewall should:

- Allow only desired connections to pass through;
- Block other requests; and
- Hide the network topology (hardware and software components) from outside networks.

The AASIS firewall is inadequate. This situation makes AASIS servers vulnerable to unauthorized access, including the server hosting AASIS financial data.

We recommend a complete firewall system be implemented that allows only necessary network traffic to communicate with AASIS servers and hides the AASIS network topology.

UPDATE: *It appears DIS has installed an adequate firewall however due to technical errors proper firewall management was not executed for January, February and part of March 2005.*

Proper firewall management includes ensuring all changes to the firewall are properly approved and the configuration for the backup firewall matches the configuration of the primary firewall. In order to help accomplish these control functions a program is run nightly to identify the configuration that was changed for that day and to compare the configuration on the primary and secondary firewall. Failure to adequately monitor configuration changes could result in the failure of the firewall to adequately protect the State's data (which includes financial and private personnel data) and the computer equipment the data resides upon.

We recommend DIS perform periodic reviews/audits of control functions to ensure only approved configurations get updated to the firewalls and the firewalls stay synchronized.

Management Response: *DIS concurs with the above recommendation. DIS will enhance the job to* *produce output files which will be used to verify that the jobs are working normally. If the job fails or does not produce the expected output file the DIS Security group will receive an email notification. DIS has also been approved to add additional Security personnel which will increase the number of staff dedicated to implementing and monitoring statewide security services. Security positions are in the process of being advertised and recruited with a July 1, 2005 employment date.*

4. Open Ports

RECOMMENDATION: One method to safeguard a networked computer against unauthorized access is to close all unneeded ports. Computers use ports with services attached to establish and maintain a communication session with another computer. AASIS servers have several ports open that are not needed for the functioning of AASIS. This situation increases the risk that an individual could gain unauthorized access to these servers by exploiting the vulnerabilities in these open ports.

We recommend that only the ports necessary for the functioning of AASIS be open.

UPDATE: *It appears the open ports and services are necessary for the functioning of AASIS.*

5. Quality Assurance Function

RECOMMENDATION: There are numerous computer programs that have been developed to perform various functions. AASIS Financial and Human Resource personnel are responsible for testing these programs to ensure that the programs perform the functions identified in the design specification documents. However, there is no independent review (Quality Assurance Function) of the source code to determine that:

- Source code complies with the design specifications;
- When appropriate, source code has hard-coded "Authority-Check" to verify that the user of the programs has the authority to perform specific transactions; and
- Data tables accessed are in conformity with the intent of the program.

We recommend that AASIS management implement a quality assurance function to ensure that programs are adequately reviewed before being moved to the production system.

UPDATE: *The AASIS Team has developed and implemented a Quality Assurance function to ensure proper control is exercised over source code changes.*

There appears to be a clear separation of duties between the teams who modify ABAP source code (ABAP programmers), those who validate and test the changes (functional specialists/functional team leads), and those who perform the code promotions (BASIS administrators).

6. Operating System

RECOMMENDATION: Controls are inadequate to prevent or detect unauthorized modifications to the AASIS operating system. Unauthorized changes to the operating system, whether accidental or intentional, increase the risk that data and programs could be destroyed, manipulated or accessed by unauthorized individuals.

There are operating system utilities, such as Trusted Computing Base, which could be used to detect penetrations and configuration changes to the operating system. These utilities store information about files, which can later be used to verify that the files have not been modified.

We recommend that these operating system utilities be used on a periodic basis to detect unauthorized changes to the operating system configuration.

There are no formal procedures for authorizing and approving changes to the operating system. In addition there is no system in place to prevent unauthorized changes to the operating system.

We recommend implementation of change control procedures to ensure that only authorized and documented changes are made to the operating system.

UPDATE: *DIS has added sufficient compensating controls and procedures to reasonably ensure the integrity of the operating system.*

7. Network Scanning

RECOMMENDATION: One function of proper network management is to identify vulnerabilities in the network devices and software. Failure to identify these vulnerabilities on a timely basis could expose the network devices to unauthorized access. DIS does receive software security updates from the major vendors that support the AASIS network. However, DIS does not use network scanning software to search for vulnerabilities that could result from a missed update or improper configuration of a network device or software. Network scanning software automatically searches for vulnerabilities that could be the result of improper configuration or missed software updates.

We recommend that DIS management use network scanning software on a periodic basis to identify network vulnerabilities.

UPDATE: *DIS has implemented periodic network scanning with adequate procedures to follow up on identified vulnerabilities.*

8. User Passwords

RECOMMENDATION: Some communication methods are utilized that send a user's ID and password over the network in clear text format. This situation could allow an individual to gain knowledge of another user's ID and password. Proper security over AASIS cannot be assured if users are able to gain knowledge of other users' passwords.

We recommend AASIS management use some form of encryption to protect passwords and other sensitive information.

UPDATE: *DIS uses encryption where appropriate when communicating with AASIS servers and other network devices.*

9. Intrusion Detection

RECOMMENDATION: One function of proper network management is to monitor network traffic to identify suspicious activity that might indicate an intrusion or attack on the network. There is some manual monitoring of network traffic, but AASIS does not have an automated system to identify possible intrusions. The volume of network traffic makes manual monitoring ineffective, thus increasing the risk that an intrusion or attack on AASIS could go undetected.

We recommend that AASIS management install an automated intrusion detection system.

UPDATE: *DIS is in the early stages of implementing an automated intrusion detection system. Completed installation and configuration is expected in the summer of 2005. If properly implemented and maintained this intrusion detection system could allow effective monitoring of the State's network for intrusions and attacks.*

Periodic network penetration testing is one method to determine if security strategies employed to protect network devices are functioning adequately to prevent or detect an intrusion or an attack. DIS does not perform formal network penetration testing. Failure to perform formal network penetration testing increases the risk that an intrusion or an attack on the network could be committed.

We recommend DIS continue implementation and configuration of the intrusion detection system. We also recommend DIS perform periodic formal network penetration testing.

Management Response: *DIS concurs with the above recommendation. DIS is in the implementation phase of configuring the Cisco – MARS (Mitigation and Response System) devices noted above that will be used to turn raw network and security data into information used to subvert real security incidents. Production deployment of the devices is 6/30/2005.*

DIS concurs with the above recommendation to run network penetration testing. DIS will implement a process and procedure for network penetration testing for DIS Hosted Services which will include more than the AASIS System. The first network penetration test will be conducted on September 1, 2005.

10. Logon ID's

RECOMMENDATION: There are several active logon IDs belonging to users who are no longer AASIS contractors or employees of the State. Sound security principles dictate that only individuals currently working on AASIS have the ability to access AASIS.

We recommend that periodic reviews be performed to ensure that only authorized individuals have the ability to access AASIS.

UPDATE: *AASIS staff performs weekly periodic reviews to ensure only current employees or contractors have access to AASIS.*

11. AASIS Transactions

RECOMMENDATION: The following AASIS transactions are typically reserved for system administrators:

- SM49 – allows execution of external operating system commands;
- SCC4 – controls change and transport ability of configuration changes in each client;
- PFCG – assigns access abilities to users (profile generator);
- STMS – enables a configuration change to be transported from one client to another;
- SU01 – User account maintenance;
- SU02 – User profile maintenance; and
- SU03 – User authorization maintenance.

Improper use of these transactions could cause incorrect processing and permit errors in the system. Numerous users, who are not system administrators, have the ability to execute these transactions.

We recommend that users have the ability to execute only those transactions necessary to perform assigned duties

UPDATE: *Our testing indicated the appropriate AASIS support staff have update access to these transactions.*

12. Operating System Logon

RECOMMENDATION: AASIS operating system logon and password usage controls have not been established for the following parameters:

- Minimum length of password;
- Minimum number of non-alpha characters in a password;
- Minimum number of alpha characters in a password;
- Maximum number of weeks a password is valid;
- Number of invalid login attempts before lockout; and
- Number of weeks before a password can be reused.

Failure to establish proper logon and password usage controls increases the likelihood that an unauthorized person could gain access to the operating system.

We recommend the establishment of logon and password controls for the above-listed parameters.

UPDATE: *The current operating system password usage controls appear to be adequate.*